UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,188	07/30/2001	Keith Alexander Harrison	30003040-2	2580

7590 04/21/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
SCHUBERT, KEVIN R

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/918,188	HARRISON ET AL.
	Examiner	Art Unit
	Kevin Schubert	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 April 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1,2,7-17,21,22,25-37,39-43,48,49,51-59 and 63</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1,2,7-17,21,22,25-37,39-43,48,49,51-59 and 63</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claims 1-2,7-17,21-22,25-37,39-43,48-49,51-59, and 63 have been considered.

Claim Objections

5   Claim 57 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 63. When

two claims in an application are duplicates or else are so close in content that they both cover the same

thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as

being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

10   *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as
> set forth in section 102 of this title, if the differences between the subject matter sought to be
15   patented and the prior art are such that the subject matter as a whole would have been obvious
> at the time the invention was made to a person having ordinary skill in the art to which said
> subject matter pertains. Patentability shall not be negatived by the manner in which the invention
> was made.

20   Claims 54-56 and 58-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan,

U.S. Patent No. 6,378,070, in view of Toyoda, U.S. Patent No. 6,335,966.

As per claims 54-56 and 58-59, the applicant describes a method of delivering a digital document

from a first station via a communications network to an intended recipient at a second station comprising

25   the following limitations which are met by Chan in view of Toyoda:

a) obtaining details of the intended recipient, including an independently verifiable data record of

the intended recipient at the first station (Chan: Col 6, line 20- Col 7, line 51);

b) determining prior to transmission of the document whether the second station is one which is

arranged to stop a transmitted document from being released until the intended recipient has proved their

30   identity, wherein the first station is configured to alternatively transmit the document as a non-encrypted

transmission when the second station is determined to not be capable of stopping a transmitted

document from being released until the intended recipient has proved their identity (Chan: Col 6, line 20-

Col 7, line 51; Toyoda: Col 10, line 61 to Col 11, line 41, Figs 9-10);

      c) transmitting the document to the second station prior to receiving proof of an intended

5   recipient's identity (Chan: Col 6, line 20- Col 7, line 51);

      d) transmitting the independently verifiable data record of the intended recipient to the second

station (Chan: Col 6, line 20- Col 7, line 51);

      e) receiving and securely retaining the transmitted document at the second station prior to

receiving proof of the intended recipient's identity and receiving the data record at the second station

10   (Chan: Col 6, line 20- Col 7, line 51);

      f) obtaining a first identifying token of an intended recipient at the second station (Chan: Col 6,

line 20- Col 7, line 51);

      g) requesting proof of the intended recipient's identity at the second station using the transmitted

independently verifiable data record (Chan: Col 6, line 20- Col 7, line 51);

15   h) releasing the document to the intended recipient when the intended recipient has proved their

identity using a second identifying token related to the first identifying token (Chan: Col 6, line 20- Col 7,

line 51).

      Chan discloses limitations of the above claim. However, Chan fails to disclose that a first station

is configured for transmitting a document as a non-encrypted transmission when a second station is not

20   configured for decryption. Toyoda discloses that a first fax station may be configured for transmitting a

document as a non-encrypted transmission when a second station is not configured for decryption. It

would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine

the ideas of Toyoda with those of Chan because doing so makes the system more robust by allowing for

communication opportunities with devices not requiring proof of an intended recipient's identity before

25   printout.

Claims 54-56 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Mandelbaum, European Patent Application Publication No. 0671830 A2, in view of Toyoda, U.S. Patent

No. 6,335,966.

5   As per claim 54, the applicant describes a method of delivering a digital document from a first

station via a communications network to an intended recipient at a second station comprising the

following limitations which are met by Mandelbaum in view of Toyoda:

          a) obtaining details of the intended recipient, including an independently verifiable data record of

the intended recipient at the first station (Mandelbaum: Col 5, lines 5-11);

10   b) determining prior to transmission of the document whether the second station is one which is

arranged to stop a transmitted document from being released until the intended recipient has proved their

identity, wherein the first station is configured to alternatively transmit the document as a non-encrypted

transmission when the second station is determined to not be capable of stopping a transmitted

document from being released until the intended recipient has proved their identity (Mandelbaum: Col 5,

15   lines 5-11; Toyoda: Col 10, line 61 to Col 11, line 41, Figs 9-10);

          c) transmitting the document to the second station prior to receiving proof of an intended

recipient's identity (Mandelbaum: Col 5, lines 29-33);

          d) transmitting the independently verifiable data record of the intended recipient to the second

station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

20   e) receiving and securely retaining the transmitted document at the second station prior to

receiving proof of the intended recipient's identity and receiving the data record at the second station

(Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

          f) obtaining a first identifying token of an intended recipient at the second station (Mandelbaum:

Col 6, lines 40-44; Col 2, lines 9-26);

25   g) requesting proof of the intended recipient's identity at the second station using the transmitted

independently verifiable data record (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

h) releasing the document to the intended recipient when the intended recipient has proved their

identity using a second identifying token related to the first identifying token (Mandelbaum: Col 6, lines

40-44; Col 2, lines 9-26).

Mandelbaum discloses limitations of the above claim. However, Mandelbaum fails to disclose

5   that a first station is configured for transmitting a document as a non-encrypted transmission when a

second station is not configured for decryption. Toyoda discloses that a first fax station may be

configured for transmitting a document as a non-encrypted transmission when a second station is not

configured for decryption. It would have been obvious to one of ordinary skill in the art at the time the

invention was filed to combine the ideas of Toyoda with those of Mandelbaum because doing so makes

10   the system more robust by allowing for communication opportunities with devices not requiring proof of an

intended recipient's identity before printout.

As per claim 55, the applicant describes the method according to claims 54, which is met by

Mandelbaum in view of Toyoda, with the following limitation which is also met by Mandelbaum:

15   Further comprising obtaining details of the intended recipient including the independently

verifiable data record prior to transmitting the document (Mandelbaum: Col 5, lines 5-27).

As per claims 56, the applicant describes the method according to claim 55, which is met by

Mandelbaum in view of Toyoda, with the following limitation which is also met by Mandelbaum:

20   Wherein the step of obtaining details comprises obtaining the independently verifiable data record

from a central database storing many possible intended recipients' details (Mandelbaum: Col 5, lines 9-

11).

As per claim 58, the applicant describes the method of claim 54, which is met by Mandelbaum in

25   view of Toyoda, with the following limitation which is also met by Mandelbaum:

Further comprising encoding the document prior to transmitting it to the second station and

decoding the received document once the intended recipient has proven their identity (Mandelbaum: Col

5, lines 33-40; Col 7, lines 27-44).

5   Claim 1-2,8-10,13-17,22,41-43,48-49, and 51-53 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Chan, U.S. Patent No. 6,378,070, in view of Nishiwaki, U.S. Patent No. 5,602,973.

As per claims 1-2,8-10,13-17,22,41-43,48-49, and 51-53, the applicant describes a method of

delivering a digital document to an intended recipient comprising the following limitations which are met

10   by Chan in view of Nishiwaki:

a) receiving and securely retaining a transmitted document at the printout station (Chan: Col 7,

lines 8-50);

b) receiving an independently verifiable data record of the intended recipient at the printout

station (Chan: Col 7, lines 8-10);

15   c) obtaining a first token of the intended recipient (Chan: Col 7, lines 8-10);

d) requesting proof of the intended recipient's identity at the printout station using data in the

independently verifiable data record of the intended recipient (Chan: Col 7, lines 8-10);

e) releasing the document when the intended recipient has proved their identity by use of a

second token that is uniquely related to the first token, wherein the retaining step comprises printing out

20   the document as received and placing it in a locked compartment and the releasing step comprises a

controller unlocking the compartment where the printed copy of the document is stored (Nishiwaki: Col 2,

lines 6-46).

Chan discloses all the limitations of the above claim, except for printing out the document and

placing it in a locked compartment. This idea is disclosed by Nishiwaki. Combining Nishiwaki into the

25   system allows the document to be printed out and placed in a locked compartment. It would have been

obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of

Nishiwaki with those of Chan because doing so furthers security in the system by incorporating the use of

a locked compartment to heighten security in the system.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan in view of Nishiwaki

5   in further view of Menezes (Menezes, Alfred J. Handbook of Applied Cryptography. CRC Press.

Washington DC. 1997. pages 452-454).

As per claim 7, the applicant describes the method according to claim 1, which is met by Chan in

view of Nishiwaki, with the following limitation which is met by Menezes:

10   Wherein the requesting step comprises requesting supply of data encoded with the second token

which can be decoded with the first token (Menezes: pages 452-454);

Chan in view of Nishiwaki discloses all the limitations of claim 1. Chan in view of Nishiwaki also

discloses that the user proves his identity by providing supply of data when the document store receives

identity information read by the smart card reader and forwarded by the printer (Col 7, lines 1-7).

15   However, Chan in view of Nishiwaki does not disclose that the supply of data is encoded with the

second token (private key) and decoded with the first token (public key). Menezes discloses the idea of a

digital signature. It would have been obvious to one of ordinary skill in the art at the time the invention

was filed to combine the ideas of Menezes with those of Chan in view of Nishiwaki and digitally sign the

supply of data with the private key because doing so provides a more secure way to authenticate the

20   identity of the user.

Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan in view

of Nishiwaki in further view of Schneier (Schneier, Bruce. Applied Cryptography. 1996. John Wiley &

Sons, Inc. Second Edition. Pages 68-73, 575-576).

25

As per claims 11 and 12, the applicant describes the method of claim 1, which is met by Chan in

view of Nishiwaki, with the following limitation which is met by Schneier:

セ

Wherein the intended recipient's independently verifiable data record is provided as an intended

recipient's digital certificate (Schneier: pages 575-576);

Chan in view of Nishiwaki discloses all the limitations of claim 1. However Chan in view of

Nishiwaki does not discloses that the independently verifiable data record is a digital certificate.

5   Schneier discloses that a certificate can be transmitted between users to verify. It would have

been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of

Schneier with those of Chan in view of Nishiwaki and have a certificate sent as an additional

independently verifiable data record so that further verification can be provided and/or a public key of a

user can be extracted.

10

Claims 21,25-37, and 39-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Chan in view of Carman, U.S. Patent No. 6,272,632.

As per claims 21,25-37, and 39-40, the applicant describes a method of delivering a digital

15   document to an intended recipient at a printout station comprising the following limitations which are met

by Chan in view of Carman:

a) obtaining a first token of each intended recipient that belong to the group of intended recipients

(Chan: Col 7, lines 8-50; Carman: Col 19, line 62 to Col 20, line 3);

b) encoding the digital document with a session key using a lightweight symmetric cryptographic

20   encryption algorithm, and encrypting the session key with the first token using an encryption algorithm

that is more computationally intensive than the symmetric cryptographic encryption algorithm (Chan: Col

7, lines 8-50);

c) receiving and securely retaining the digital document, the encrypted session key and an

independently verifiable data record of each intended recipient (Chan: Col 7, lines 8-50);

25   d) requesting proof of each intended recipient's identity at the printout station using data in the

independently verifiable data record of the intended recipient (Chan: Col 7, lines 8-50);

e) receiving proof of each intended recipient's identity in the form of a second token uniquely

related to the first token (Chan: Col 7, lines 8-50);

f) decrypting the encrypted session key with the second token, decoding the digital document with

the decrypted session key, and releasing the document (Chan: Col 7, lines 8-50);

5   g) the receiving step comprises receiving a plurality of transmitted independently verifiable data

records of the intended recipients at the printout station (Chan: Col 7, lines 8-50);

h) the obtaining step comprises obtaining the first tokens of each of the intended recipients in the

group of intended recipients (Chan: Col 7, lines 8-50);

i) the requesting step comprises requesting proof of each of the intended recipients' identities at

10   the printout station using data in the independently verifiable data records of the intended recipients

(Chan: Col 7, lines 8-50);

j) the processing step comprises processing each of the intended recipients' response to the

request and releasing the document when all of the intended recipients have proved their identity by use

of respective second tokens that are each uniquely related to respective ones of the first tokens (Chan:

15   Col 7, lines 8-50);

Chan discloses the above limitations with the exception that Chan does not disclose obtaining a

plurality of first tokens. Chan discloses obtaining only a first token of a single recipient. Carman

discloses the idea of obtaining a plurality of first tokens (public keys) to encrypt a message so that a

plurality of entities are necessary to play a part in the decryption. Combining the ideas of Carman with

20   Chan allows for a message to be encrypted in more than one first token. It would have been obvious to

one of ordinary skill in the art at the time the invention was filed to combine the ideas of Carman with

those of Chan for the purpose of creating an environment which is more secure because it depends on

more than one entity providing verification for a received message.

25   Claims 57 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan in view

of Toyoda in further view of Schneier.

As per claims 57 and 63, the claims are rejected under Chan in view of Toyoda in further view of Schneier for the same reasons given in the rejection of claim 12.

Claims 1-2,5-11,13-17,41-43,46-48,54-56, and 58 are rejected under 35 U.S.C. 103(a) as being
5   unpatentable by Mandelbaum in view of Nishiwaki.

As per claims 1,41, and 49, the applicant describes a method of delivering a digital document to an intended recipient at a printout station comprising the following limitations which are met by Mandelbaum in view of Nishiwaki:

10   a) receiving and securely retaining a transmitted document at the printout station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

       b) receiving an independently verifiable data record of the intended recipient at the printout station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-26);

       b) obtaining a first token of the intended recipient (Mandelbaum: Col 2, lines 50-53);

15   c) requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient (Mandelbaum: Col 6, lines 56-58; Col 7, lines 1-6; Col 5, lines 49-58; Table 10 of Fig 4);

       d) releasing the document when the intended recipient has proven their identity by use of a second token that is uniquely related to the first token, wherein the retaining step comprises printing out

20   the document as received and placing it in a locked compartment and the releasing step comprises a controller unlocking the compartment where the printed copy of the document is stored (Mandelbaum: Col 7, lines 27-47; Nishiwaki: Col 2, lines 6-46);

       Mandelbaum discloses all the limitations of the above claim, except for printing out the document and placing it in a locked compartment. This idea is disclosed by Nishiwaki. Combining Nishiwaki into

25   the system allows the document to be printed out and placed in a locked compartment. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of

Nishiwaki with those of Mandelbaum because doing so furthers security in the system by incorporating

the use of a locked compartment to heighten security in the system.

As per claims 2 and 42, the applicant describes the method of claims 1 and 41, which are

5   anticipated by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by

Mandelbaum:

Wherein the transmitted document is a fax document and the printout station comprises a fax

machine (Col 3, lines 15-17).

10   As per claim 7, the applicant describes a method according to claim 1, which is anticipated by

Mandelbaum in view of Nishiwaki, with the following limitation which is also met by Mandelbaum:

Wherein the requesting step comprises requesting supply of data encoded with the second token

which can be decoded with the first token (Col 4, lines 11-21).

15   As per claim 8, the applicant describes the method of claim 1, which is anticipated by

Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step is carried out when the intended recipient has presented a portable

data carrier holding the second token to the printout station and has transferred data to prove their

identity (Col 7, lines 27-56).

20

As per claims 9 and 48, the applicant describes the method of claims 8 and 41, which are met by

Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step further comprises the intended recipient entering a verifiable security

identifier into the printout station to establish that they are the legitimate owner of the portable data carrier

25   (Col 4, lines 21-24).

As per claim 10, the applicant describes the method of claim 8, which is met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the portable data carrier is a smart card and the printout station comprises a smart card reader (Col 4, lines 9-13).

5

As per claim 11, the applicant describes the method of claim 1, which is met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Wherein the obtaining step comprises extracting the first token transmitted with the document and the data record (Table 404 of Fig 4);

10   As one can see in the table, the fax machine is able to extract information about the first token from the message and display the information as a flag which is set when the message is encrypted with the intended recipient's public key.

As per claim 13, the applicant describes the method of claim 1, which is met by Mandelbaum in

15   view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Further comprising carrying out an on-line check of the validity of the intended recipient's independently verifiable data record (Col 4, lines 17-24);

The applicant writes that the smart card authentication method is preferably the AT&T CSS user authentication system "in which the user calls the system" (Col 4, lines 17-19). Since the user is calling

20   the system for authentication, an online authentication is taking place.

As per claim 14, the applicant describes the method of claim 1, which is met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

Further comprising instructing a third party to carry out an on-line check of the validity of the

25   intended recipient's independently verifiable data record (Col 4, lines 17-24);

Since the authentication system is one in which the user calls into the system, it is reasonable to assume that a third party validates the intended recipient.

As per claims 15 and 16, the applicant describes the method of claims 13 and 14, which are met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by Mandelbaum:

5   Wherein the releasing step further comprises only releasing the document if the validity of the independently verifiable data record has been confirmed as a result of the check (Col 4, lines 23-24).

As per claims 17,43, and 51-53, the applicant describes the method of claims 1,41, and 49, which are met by Mandelbaum in view of Nishiwaki, with the following limitation which is also anticipated by

10   Mandelbaum:

Wherein the first and second tokens comprise private and public encryption/decryption keys of the intended recipient (Col 2, lines 50-53; Col 7, lines 27-32);

The use of the recipient's public key, or first token, is described (Col 2, lines 50-53) as well as the use of the intended recipient's private key, or second token, (Col 7, lines 27-32).

15

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Nishiwaki in view of Schneier.

As per claim 12, the applicant describes the method of claim 11, which is met by Mandelbaum in

20   view of Nishiwaki, with the following limitation which is met by Schneier:

Wherein the intended recipient's independently verifiable data record is provided as an intended recipient's digital certificate (Schneier: pages 575-576);

Mandelbaum in view of Nishiwaki discloses all the limitations of claim 1. Mandelbaum in view Nishiwaki does not disclose certificate being sent as an independently verifiable data record.

25   Schneier discloses that a certificate can be transmitted between users for verification. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneir with those of Mandelbaum in view of Nishiwaki and have a certificate sent as an

additional independently verifiable data record so that further verification can be provided and/or a public

key of a user can be extracted.

Claims 21-22,25-37, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over

5   Mandelbaum in view of Schneier in further view of Carman, U.S. Patent No. 6,272,632.

As per claim 21, the applicant describes a method of delivering a digital document to an intended

recipient at a printout station comprising the following limitations which are met by Mandelbaum in view of

Schneier in further view of Carman:

10   a) obtaining a first token of each intended recipient that belong to the group of intended recipients

(Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53; Carman: Col 19, line 62 to Col 20, line 3);

b) encoding the digital document with a session key using a lightweight symmetric cryptographic

encryption algorithm, and encrypting the session key with the first token using an encryption algorithm

that is more computationally intensive than the symmetric cryptographic encryption algorithm (Schneier:

15   page 33);

c) receiving and securely retaining the digital document, the encrypted session key and an

independently verifiable data record of each intended recipient (Mandelbaum: Col 6, lines 40-44; Col 2,

lines 9-53);

d) requesting proof of each intended recipient's identity at the printout station using data in the

20   independently verifiable data record of the intended recipient (Mandelbaum: Col 6, lines 40-44; Col 2,

lines 9-53);

e) receiving proof of each intended recipient's identity in the form of a second token uniquely

related to the first token (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

f) decrypting the encrypted session key with the second token, decoding the digital document with

25   the decrypted session key, and releasing the document (Mandelbaum: Col 6, lines 40-44; Schneier: page

33);

g) the receiving step comprises receiving a plurality of transmitted independently verifiable data

records of the intended recipients at the printout station (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-

53);

h) the obtaining step comprises obtaining the first tokens of each of the intended recipients in the

5   group of intended recipients (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

i) the requesting step comprises requesting proof of each of the intended recipients' identities at

the printout station using data in the independently verifiable data records of the intended recipients

(Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

j) the processing step comprises processing each of the intended recipients' response to the

10   request and releasing the document when all of the intended recipients have proved their identity by use

of respective second tokens that are each uniquely related to respective ones of the first tokens

(Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53);

Mandelbaum discloses the above limitations with the exception that Mandelbaum does not

disclose the use of encrypting a session key with a first token. Schneier discloses encrypting a session

15   key with a first token in order to establish secure communication through the session key. It would have

been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of

Schneier with those of Mandelbaum and utilize a session key because doing so enhances security in the

system.

Mandelbaum in view of Schneier does not disclose obtaining a plurality of first tokens.

20   Mandelbaum in view of Schneier discloses obtaining only a first token of a single recipient. Carman

discloses the idea of obtaining a plurality of first tokens (public keys) to encrypt a message so that a

plurality of entities are necessary to play a part in the decryption. Combining the ideas of Carman with

Mandelbaum in view of Schneier allows for a message to be encrypted in more than one first token. It

would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine

25   the ideas of Carman with those of Mandelbaum in view of Schneier for the purpose of creating an

environment which is more secure because it depends on more than one entity providing verification for a

received message.

As per claims 22 and 25-37, the applicant describes the method of claim 21, which is met by

Mandelbaum in view of Schneier in further view of Carman, with the following limitation which is met by

Mandelbaum:

5   Wherein the transmitted document is a fax document and the printout station comprises a fax

machine (Mandelbaum: Col 6, lines 40-44; Col 2, lines 9-53).

As per claim 39, the applicant describes the method of claim 21, which is anticipated by

Mandelbaum in view of Schneier in view of Carman, with the following additional limitation which is also

10   met by Schneier:

Wherein the transmitted document or a session encryption/decryption key of the transmitted

document has been sequentially encrypted with each of the first tokens of the intended recipients in a

given order and the processing step comprises sequentially decrypting the transmitted document or a

session encryption/decryption key with each of the second tokens of the intended recipients in the

15   reverse of the given sequential order (Col 19, line 62 to Col 20, line 3).

Claims 57 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum

in view of Toyoda in further view of Schneier.

20   As per claims 57 and 63, the claims are rejected under Mandelbaum in view of Toyoda in further

view of Schneier for the same reasons given in the rejection of claim 12 (see above).

Claims 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in

further view of Carman.

25

As per claim 40, the applicant describes a method of delivering a digital document which is met by Mandelbaum (see the rejection for claim 1) with the additional limitation of incorporating the use of a plurality of intended recipients which is met by Carman (Col 19, line 62 to Col 20, line 3).

5   Claim 59 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Toyoda in further view of Auerbach, European Patent Application Publication No. 0798892 A2.

As per claim 59, the applicant describes the method of claim 58, which is met by Mandelbaum, with the following limitation which is met by Auerbach:

10   Wherein the encoding/decoding steps comprise using enveloping encryption/decryption techniques (Auerbach: Col 3, lines 5-10; Col 3, lines 26-30);

Mandelbaum in view of Toyoda describes all the limitations of claim 58. However, Mandelbaum in view of Toyoda fail to disclose the use of enveloping encryption and decryption techniques.

Auerbach discloses a method for the creation and distribution of digital documents using the

15   methods and techniques of secure cryptographic envelopes (Col 1, lines 3-8). Cryptographic envelopes provide an extra layer of security for messages because they comprise superencrypting a message. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Auerbach with those of Mandelbaum in view of Toyoda so that the transmitted message is encoded using enveloping technique for extra security.

20

Response to Arguments

Applicant's arguments, see Remarks, filed 4/5/06, with respect to the 112, first paragraph, rejection of claims 64-65 have been fully considered and are persuasive. The 112, first paragraph, rejection of claims 64-65 has been withdrawn.

25

Applicant's arguments with respect to the 112, second paragraph, rejection of claims 21 and 63 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn.

Applicant's arguments with respect to the 102(e) and 102(b) rejections of claim 54 et al under

Chan and Mandelbaum have been fully considered but are moot in view of the new ground(s) of rejection.

5   Applicant's arguments with respect to the 103(a) rejections of claim 1 et al under Chan in view of

Nishiwaki have been fully considered, but they are not persuasive. Applicant presents the following

arguments:

          1) Chan fails to disclose claim 1 part a) because the processes of Chan cannot be co-located

          2) Nishiwaki fails to disclose that an intended recipient provides proof of his identity and therefore

10   claim 1 part e) is not met

          Examiner respectfully disagrees. Regarding 1), Examiner submits that the processes can be co-

located as indicated by Chan (Col 8, lines 30-34). Further, even if Applicant's assertion were correct,

Examiner fails to see how such an argument precludes claim 1 part a) from being met.

15   Regarding 2), Examiner submits that Nishiwaki discloses that a printout device may enact

security by requiring a recipient to enter an appropriate authorization identification to unlock a bin and

receive a printout (Col 2, lines 35-43). Accordingly, Applicant's arguments are not persuasive.

          Applicant's arguments with respect to the 103(a) rejection of claim 1 et al under Mandelbaum in

20   view of Nishiwaki have been fully considered, but they are not persuasive. In addition to presenting the

Nishiwaki argument discussed above, Applicant presents the following argument:

          1) motivation

          Examiner disagrees. Specifically, Applicant argues that a user must be present at a print unit for

25   a document to be printed. Even if true, motivation still exists for combining Nishiwaki into the system

because doing so furthers security by also requiring a user to submit an identification code.

Applicant's arguments with respect to the 103(a) rejection of claims 21,25-37, and 39 under Chan in view of Carman have been fully considered but are not persuasive. Applicant presents the following argument:

1) Chan fails to disclose claim 21 part c) because the processes of Chan cannot be co-located

5   2) Chan fails to disclose that a document is retained at the printout station such that it is released after an intended recipient or group of intended recipients proves their identity

3) Nishiwaki or Chan fail to disclose parts d), e), and f)

4) Carman does not teach the particular claimed printing approach

10   Examiner respectfully disagrees. Regarding 1), such an argument has already been addressed with regard to claim 1.

With regard to 2), Examiner disagrees but fails to see which claim language applicant is referring to for his argument. Examiner believes the argument may be moot and outside the scope of the claims. Examiner respectfully requests that Applicant indicate which claim language he refers to as deficient in

15 the instant combination.

With regard to 3), Examiner notes that the argument in light of Nishiwaki is moot in light of the fact that the instant rejection of claim 1 is a 103(a) rejection under Chan in view of Carman. Accordingly, Applicant's arguments with respect to Nishiwaki are moot. Further, Applicant's argument that Chan does not disclose parts d), e), and f), fails to comply with 37 CFR 1.111(b) because it amounts to a general

20 allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

With regard to 4), Examiner notes that Carman is not relied on to teach the particular claimed printing approach. The combination of Chan in view of Carman meets the particular claimed approach, and Examiner's reliance on each reference is indicated in the rejection of claim 21. Accordingly, this

25 argument is moot.

Applicant's arguments with respect to the 103(a) rejection of claims 21-37 and 39 under

Mandelbaum in view of Schneier in further view of Carman fail to comply with 37 CFR 1.111(b) because

they amount to a general allegation that the claims define a patentable invention without specifically

pointing out how the language of the claims patentably distinguishes them from the references.

5

Applicant's arguments with respect to the 103(a) rejection of claims 41-43,48-49, and 51-53

under Chan in view of Nishiwaki have been fully considered, but they are not persuasive. Applicant's

argument that Nishiwaki does not teach providing proof of a recipient's identity has been addressed with

respect to the rejection of claim 1 (see above).

10

Applicant's arguments with respect to the 103(a) rejection of claims 41-43,48-49, and 51-53

under Mandelbaum in view of Nishiwaki have been fully considered, but they are not persuasive.

Applicant's argument that there is no motivation for combination has been addressed with respect to the

rejection of claim 1 (see above).

15

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office

action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of

the extension of time policy as set forth in 37 CFR 1.136(a).

20   A shortened statutory period for reply to this final action is set to expire THREE MONTHS from

the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date

of this final action and the advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on the date the advisory action

is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

25   the advisory action. In no event, however, will the statutory period for reply expire later than SIX

MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

5   Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through

10   Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

15   KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

20